

⑫ 公開特許公報(A)

昭63-311493

⑤ Int. Cl.⁴

識別記号

庁内整理番号

⑬ 公開 昭和63年(1988)12月20日

G 06 K 17/00

G 06 F 15/21

G 07 F 7/08

3 4 0

T-6711-5B

B-7230-5B

C-6929-3E

審査請求 未請求 発明の数 1 (全4頁)

⑭ 発明の名称 電子カードシステム

⑮ 特 願 昭62-146852

⑯ 出 願 昭62(1987)6月15日

⑰ 発 明 者 上 林 弘 明 神奈川県秦野市堀山下1番地 株式会社日立製作所神奈川工場内

⑱ 出 願 人 株式会社日立製作所 東京都千代田区神田駿河台4丁目6番地

⑲ 代 理 人 弁理士 武 顕 次郎 外1名

明 細 書

1. 発明の名称

電子カードシステム

2. 特許請求の範囲

1. 磁気ストライプあるいはICメモリ等の記録媒体を持つ電子カードを用いる電子カードシステムにおいて、該電子カード発行時、該電子カードに初期暗証番号を前回取引時点の暗証番号として記録し、該電子カードと取引するホストコンピュータあるいは端末システム内に、取引毎に次の取引を可能とする前記暗証番号の更新条件を登録し、ホストコンピュータあるいは端末システムは、取引時に入力された暗証番号と、前記電子カード内に記録されている前回取引時点の暗証番号を用い、前記暗証番号の更新条件により算出した今回の暗証番号とを比較することにより取引の正当性を確認し、取引終了後、今回取引の暗証番号を前回取引時点の暗証番号として前記電子カードに記録することを特徴とする電子カードシステム。

3. 発明の詳細な説明

〔産業上の利用分野〕

本発明は、リード、ライト可能な電子カードを用いる取引システムに係り、特に不正入手カード、贋カードのいずれを用いた不正取引をも防止することが可能な電子カードシステムに関する。

〔従来の技術〕

近年、電子カードを利用する取引が益々増大しており、それに伴い、不正カードによる不正取引の割合が増加し、不正取引による損害も多くなっている。電子カードを利用する不正取引としては、不正入手したカードより暗証番号を取出し、この暗証番号を用いて不正取引を行う場合と、任意の暗証番号を記録した贋カードを作成して不正取引を行う場合とに大別される。

このような不正取引を防止するための従来技術として、例えば、特開昭57-111760号公報に「データ処理装置」として記載された技術が知られている。この従来技術は、取引コードとして従来の暗証番号等の固定情報と、前回取引の月日等

の変動情報とを組合わせ、カード読取装置のキーボードからこれらの情報を取引コードとして入力し、固定情報と変動情報の両方を比較確認することにより不正取引の防止を図るものである。また、他の従来技術として、特開昭59-99573号公報に「コンピュータの入力装置」として記載された技術が知られている。この従来技術は、前述の場合と同様に、固定情報と変動情報とを用いるが、この技術の場合には、固定情報と変動情報とを、電子カード及びコンピュータ側の双方に記録保持し、カード利用時に、これらの両情報と比較することにより不正取引の防止を図るものである。さらに、他の従来技術として、特開昭59-186081号公報に「取引者の認証方式」として記載された技術が知られている。この従来技術は、前述と同様な変動情報を、取引残高、処理通番、乱数等を用いた所定の演算式により演算して、その結果をその時々の取引コードにおける変動情報として用いることにより、不正取引の防止を図るものである。

自に、ホストコンピュータあるいは端末システムに登録保持させ、取引時、ホストコンピュータあるいは端末システムの側で前記登録済のアルゴリズムに基づいて、今回の取引暗証番号を生成することにより、暗証番号そのものをダイナミックに変動させることにより達成される。

〔作用〕

電子カードを利用して取引を行う場合、取引に先立つて、暗証番号を変更するための暗証番号アルゴリズムを、取引者独自にホストコンピュータあるいは端末システムに初期登録し、取引の都度、暗証番号そのものを変動させ、今回取引の暗証番号を当該電子カードに記録更新する。次の取引時、利用者は、前回の暗証番号と登録してあるアルゴリズムにより変更した暗証番号を用いて取引を行い、ホストコンピュータあるいは端末システムは、電子カードに記録されている前回使用の暗証番号と、登録されているアルゴリズムにより今回用いられるはずの暗証番号を演算し、端末より入力される暗証番号と、演算した暗証番号とを比較する

〔発明が解決しようとする問題点〕

前記従来技術のうち、第1の従来技術は、不正入手カードによる不正取引を防止することは可能であるが、贋カードによる不正取引を防止することができないという問題点を有し、第2の従来技術は、逆に贋カードによる不正取引防止には効果はあるが、不正入手カードによる不正取引防止には効果がないという問題点を有する。また、第3の従来技術は、変動情報の生成アルゴリズムを複雑にただけで、第2の従来技術の場合と同様に、贋カードによる不正取引を防止することは可能であるが、不正入力カードによる不正取引を防止することはできないという問題を有している。

本発明の目的は、前記従来技術の問題点を解決し、不正入手カード、あるいは贋カードのいずれのカードを用いた不正取引をも防止することが可能な電子カードシステムを提供することにある。

〔問題点を解決するための手段〕

本発明によれば、前記目的は、暗証番号を変動させるアルゴリズムを当該電子カード所有者が独

ことにより、正しい取引が行われているか否かの検証を行う。これによつて、たとえ、取引時に暗証番号を盗視されたとしても、この暗証番号は、次回取引には無効であり、電子カードを不正入手しても次回取引は行うことができない。また、贋カードを作成しようとしても、暗証番号生成アルゴリズムが不明であるため、贋カードを作成することができない。

〔実施例〕

以下、本発明による電子カードシステムの一実施例を図面により詳細に説明する。

第1図は本発明の一実施例の構成を示すブロック図である。第1図において、1は電子カード、2はカード読取り読み装置、3はディスプレイ装置、4はキーボード、5はホストコンピュータ、6はファイル装置、7は電子カード発行装置、8は前回取引暗証番号、9は取引メンバファイル、10は暗証番号更新条件ファイルである。

本発明による電子カードシステムは、磁気カードまたはICカード等の再読み込み可能な電子カー

ド1と、業務を行うためのキーボード4及びディスプレイ装置3が接続され、電子カード1をリードまたはライトするとともにホストコンピュータ5との間で、所定の取引を行うために必要なデータの送受信を行うカード読取り書き込み装置2と、ファイル装置6が接続されたホストコンピュータ5と、取引口座を開設する電子カード発行装置7とにより構成されている。電子カード1には、記録媒体部の所定エリアに前回取引に用いられた暗証番号8が記録される。また、ファイル装置9の所定エリアには、取引メンバファイル9と各取引メンバに対応した暗証番号更新条件ファイル10が備えられている。

このように構成された本発明の一実施例の動作を以下に説明する。

まず、取引口座を開設する場合、取引メンバは、電子カード発行装置7を用い、定められた手順により、取引メンバ番号、初期暗証番号、暗証番号の更新条件式であるアルゴリズム、その他必要情報の登録を行い、電子カード1の発行を受ける。

から入力された前回取引暗証番号8を用い、暗証番号更新条件ファイル10内の取引メンバに対応する暗証番号更新条件、すなわち更新アルゴリズムにより今回取引暗証番号を算出する。次に、ホストコンピュータ5は、この算出結果と、カード読取り書き込み装置2から入力され、ホストコンピュータ5に送られた今回取引暗証番号とを比較し、一致した場合に取引成立と判定し、以後キーボード4より入力され、カード読取り書き込み装置を介して送信される取引内容に従って、必要な取引業務を実行する。取引が完了すると、ホストコンピュータ5は、カード読取り書き込み装置2に対して、今回用いられた取引暗証番号を次の取引のために、電子カード1の前回取引暗証番号8の記録エリアに記録するよう指示して、今回の取引を終了する。

取引メンバは、前述した今回取引暗証番号を自ら記憶しておき、次の取引においては、この暗証番号と、先に登録し自ら記憶している暗証番号更新条件に基づいて次回取引時の暗証番号を計算

この場合、電子カード1の前回取引暗証番号8として、前述の初期暗証番号が記録される。また、電子カード発行装置7から登録された情報は、ホストコンピュータ5に送信され、ファイル装置6の取引メンバファイル9及び暗証番号更新条件ファイル10内に登録される。

取引メンバが最初の取引を行う場合、取引メンバは、電子カード1をカード読取り書き込み装置2に挿入し、キーボード4とディスプレイ装置3を用いて、予め、電子カード発行装置7により登録し、電子カード1に記録されている初期暗証番号を、電子カード発行装置7より登録した暗証番号更新条件としてのアルゴリズムを用いて計算し、得られた結果を今回の取引暗証番号として入力する。カード読取り書き込み装置2は、キーボード4より入力された今回の取引暗証番号と、電子カード1から読取った前回取引暗証番号8、この場合、初期暗証番号と、取引メンバ番号とをホストコンピュータ5に送信し、取引依頼を実行する。ホストコンピュータ5は、カード読取り書き込み装置2

し、計算された暗証番号を用いることにより、次の取引を正しく成立させることができる。

前述した暗証番号の更新条件は、予め定められた制約の範囲内で取引メンバが独自に決定することが可能である。例えば、初期暗証番号である4桁の数字Nに対して、 N^2 の下位4桁を次の取引の暗証番号とすることができる。あるいは、定数Cを用意し、 $N \times C$ 、 $N + C$ 等の算術結果の上位4桁を用いてもよい。これらの更新条件式は、その種類が豊富にほど、不正防止の信頼性をより向上させることができる。更新条件の与え方や、取引メンバの更新条件登録手順については、公知の技術により最適なシステムの構築が可能である。

また、不正取引が行われても被害額が小さい場合等、むしろ取引時の操作の簡便さを重視する場合には、更新条件式を $N \times 1$ とすることにより、本発明は、全く従来の認証方式と同様に、単一の変化しない暗証番号を用いるシステムとなる。

前述した本発明の実施例は、暗証番号更新条件ファイル10等を有するファイル装置6をホスト

コンピュータ 5 に備えているが、本発明は、カード読取り替込み装置 2 を含む端末システム内にファイル装置を備えるように構成してもよい。

さらに、本発明は、ホストコンピュータ側に、前回取引暗証番号を別ファイルとして保存しておき、取引時に、カード読取り書込み装置２から送信される前回取引暗証番号と保存された前回取引暗証番号とを比較するようにして、さらに信頼性の高いシステムとすることが可能である。

本発明の実施例は、前述したように、暗証番号更新条件の選び方によつて、きわめて信頼度の高い高機能の電子カードシステムとすることも、また、ごく一般的な個定の暗証番号を用いる簡易な電子カードシステムとすることもできる。

【発明の効果】

以上説明したように、本発明によれば、取引のために用いる暗証番号が電子カードそのものには直接記録保持されていないこと、暗証番号の更新条件は取引メンバーが新規に口座を開き電子カードの発行を受ける時点以外に監視されることがない

こと、第三者がホストコンピュータの暗証番号更新条件ファイルにアクセスすることができないこと等により、不正入手した電子カードあるいは偽造した腹カードを用いた不正取引をほぼ完全に近く防止することができる。

4. 図面の簡単な説明

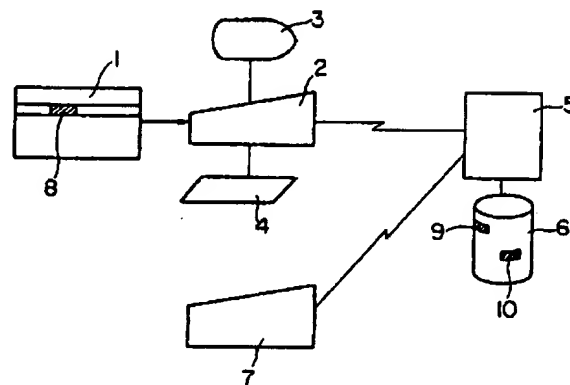
第1図は本発明の一実施例の構成を示すブロック図である。

1 …… 電子カード、2 …… カード読取り読み込み装置、3 …… ディスプレイ装置、4 …… キーボード、5 …… ホストコンピュータ、6 …… ファイル装置、7 …… 電子カード発行装置、8 …… 前回取引暗証番号、9 …… 取引メンバーファイル、10 …… 暗証番号更新条件ファイル。

代理人 弁理士 武 顯次郎（外1名）



第 1 图



- 1: 電子カード
- 2: カード読取り書込み装置
- 3: ディスプレイ
- 4: キーボード
- 5: ホストコンピュータ
- 6: ファイル装置
- 7: 電子カード発行装置
- 8: 簡易取引(暗証番号)
- 9: 取引メンバーファイル
- 10: 暗証番号更新条件ファイル